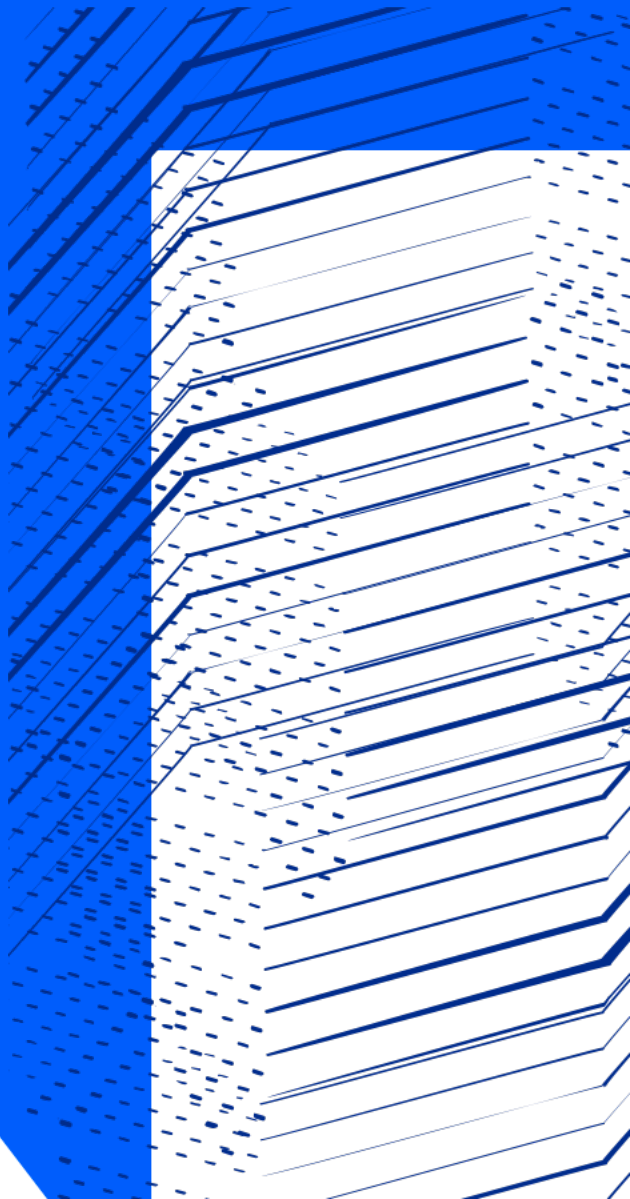
Science and Technology Facilities Council

Cybersecurity in UK digital research infrastructures

David Crooks
david.crooks@stfc.ac.uk



UKRI Digital Research Infrastructures

- Digital research and innovation infrastructure (DRI) underpins the research and innovation ecosystem.
- It enables us to solve problems, and to analyse and understand complex topics on any subject.
- This is possible because digital infrastructure allows us to work with data and computation efficiently and securely, at scale.

UKRI Science and Technology Facilities Council

What is DRI?

- The building blocks of the DRI system include:
  - large scale compute facilities, including high-throughput, high-performance, and cloud computing
  - data storage facilities, repositories, stewardship and security
  - software and shared code libraries
  - mechanisms for access, such as networks and user authentication systems
  - people: the users, and the experts who develop and maintain these powerful resources.

DRI opportunities and risks

- With its role underpinning UK research, it is vital that the DRI system be trustworthy and provide the assurance necessary to protect the assets and reputation of those using it

- DRI is often nationally or globally federated across multiple organisations
  - Often involving a heterogeneous mix of technologies
  - Driven by national and international science community needs
  - This is what makes it so different to a corporate IT infrastructure

DRI opportunities and risks

- With the open risk appetite necessary to support innovative computing infrastructures, it is vital that these risks be managed appropriately

- A key part of this process is an effective approach to cybersecurity

DRI Cybersecurity

- A new project to develop a common approach to cybersecurity across the DRI landscape
  - Essential in our current environment
  - Building on experience from leading work for research infrastructures nationally and internationally

- Aims to establish a common cybersecurity defence framework across the DRI landscape
  - an initial phase to be completed by the end of FY23

Science and Technology Facilities Council

DRI Cybersecurity Goals

- This work will focus on building trust between DRI participants to share information about ongoing incidents
  - And actively use this information in a timely fashion

- To effectively use this information we must have
  - a technical way of sharing information that supports automation
  - fine-grained monitoring, focused on network monitoring in the first instance

- The first phase of the DRI Cybersecurity project will develop these capabilities with a core of early adopters
  - Following an initial workshop in early 2023

Data integrity

- A key differentiator of national and international scale research infrastructures is ubiquitous need for very large data storage and management

- It is vital that the integrity of this data is maintained to support our national science goals

- One impact of the increase in likelihood of ransomware attacks is a threat to this data integrity
  - One aspect of sharing approaches to cybersecurity from a research perspective is sharing best practice within our community towards protecting this data

UKRI Science and Technology Facilities Council

National context

- The DRI Cybersecurity project takes place alongside existing national work
  - Jisc with a National R&E Network perspective
  - NCSC with a national and government perspective

- The perspectives shown below are complimentary and strengthen our overall ability to defend and protect our R&E community

NCSC	DRI Cybersecurity	Jisc
"We support the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public."	"Represents the perspective digital research infrastructures including innovative workflows and large-scale data management."	"Jisc is the UK digital, data and technology agency focused on tertiary education, research and innovation.."

UKRI Science and Technology Facilities Council

NCSC Cyber Assessment Framework

- Born of UK response to NIS1 *and other sources*
- GovAssure

> - All government departments and a select number of arm's length bodies to have their cyber security reviewed under new, more stringent measures.
> - The new cyber security regime, known as GovAssure, will be run by the Government Security Group, part of the Cabinet Office.
> - GovAssure delivers on a key part of the Government Cyber Security Strategy by improving cyber resilience and help government organisations protect themselves from growing hostile cyber threats.

- Will be proposed as baseline for DRI cybersecurity development
- **Mappings between this and other frameworks (ISO27k, NIST CSF, CIS, …) are absolutely vital**
- PDF | Guidance

Science and Technology Facilities Council

CAF Objectives

A. Managing security risk
B. Protecting against cyber-attack
C. Detecting cyber security events
D. Minimising the impact of cyber security incidents

Principles: Managing security risk

- Governance
- Risk Management
- Asset Management
- Supply Chain

Science and Technology Facilities Council

Principles: Protecting against cyber-attack

- Service Protection Policies and Processes
- Identity and Access Control
- Data Security
- System Security
- Resilient Networks and Systems
- Staff Awareness and Training

Principles: Detecting cyber security events

- Security Monitoring
- Proactive Security Event Discovery

Principles: Minimising impact of cyber incidents

- Response and Recovery Planning
- Lessons Learned

Science and Technology Facilities Council

Additional elements for DRI strategy

- Interoperability and alignment with international developments
  - All of the work here
  - Ongoing work on sharing threat intelligence, operational security, etc…

- In addition to “Lessons Learned” in previous objective, significant focus on maturity development and continuous improvement

- 3-5 year strategy being written for proposal this week

UKRI Science and Technology Facilities Council

Thank you

Science and Technology Facilities Council @STFC_Matters Science and Technology Facilities Council

Science and
Technology
Facilities Council

Questions?